CLAIMS

1. A method for determining computer security threats, comprising:

obtaining a possible intrusions report having indicia of a plurality of possible network intrusions;

retrieving an actual intrusions report having indicia of at least one actual intrusion from a security network, wherein the security network is at least configured to utilize at least one taxonomy;

comparing the possible intrusion reports with the actual intrusion reports to determine one or more false positives and one or more true positives; and

updating the at least one taxonomy with at least one of the false positives and at least one of the true positives.

2. The method of Claim 1, wherein the step of comparing further comprises:

labeling indicia of at least one possible network intrusion of a plurality of possible network intrusions as a false positive when at least one actual intrusion counterpart has not occurred; and

labeling indicia of the at least one possible network intrusion of the plurality of possible network intrusions as true positive when at least one actual intrusion counterpart has occurred.

3. The method of Claim 1, wherein the updating the at least one taxonomy further comprises sorting the at least one possible network intrusion of the plurality of network intrusions labeled as true positive.

4. The method of Claim 1, wherein the updating the at least one taxonomy further comprises prioritizing the at least one possible network intrusion of the plurality of network intrusions labeled as true positive.

5. An apparatus for determining computer security threats, comprising:

means for obtaining a possible intrusions report having indicia of a plurality of possible network intrusions;

means for retrieving an actual intrusions report having indicia of at least one actual intrusion from a security network, wherein the security network is at least configured to utilize at least one taxonomy;

means for comparing the possible intrusion reports with the actual intrusion reports to determine one or more false positives and one or more true positives; and

means for updating the at least one taxonomy with at least one of the false positives and at least one of the true positives.

6. The apparatus of Claim 5, wherein means for comparing further comprises:

means for labeling indicia of at least one possible network intrusion of a plurality of possible network intrusions as a false positive when at least one actual intrusion counterpart has not occurred; and

means for labeling indicia of the at least one possible network intrusion of the plurality of possible network intrusions as true positive when at least one actual intrusion counterpart has occurred.

7. The apparatus of Claim 5, wherein the means for updating the at least one taxonomy further comprises means for sorting the at least one possible network intrusion of the plurality of network intrusions labeled as true positive.

8. The apparatus of Claim 5, wherein the means for updating the at least one taxonomy further comprises means for prioritizing the at least one possible network intrusion of the plurality of network intrusions labeled as true positive.

9. A computer program product for determining computer security threats, the computer program product having a medium

with a computer product embodied thereon, the computer program comprising:

computer code for obtaining a possible intrusions report having indicia of a plurality of possible network intrusions;

computer code for retrieving an actual intrusions report having indicia of at least one actual intrusion from a security network, wherein the security network is at least configured to utilize at least one taxonomy;

computer code for comparing the possible intrusion reports with the actual intrusion reports to determine one or more false positives and one or more true positives; and

computer code for updating the at least one taxonomy with at least one of the false positives and at least one of the true positives.

10. The computer program product of Claim 9, wherein computer code for comparing further comprises:

computer code for labeling indicia of at least one possible network intrusion of a plurality of possible network intrusions as a false positive when at least one actual intrusion counterpart has not occurred; and

computer code for labeling indicia of the at least one possible network intrusion of the plurality of possible network intrusions as true positive when at least one actual intrusion counterpart has occurred.

11. The computer program product of Claim 9, wherein the computer code for updating the at least one taxonomy further comprises a computer program product for sorting the at least one possible network intrusion of the plurality of network intrusions labeled as true positive.

12. The computer program product of Claim 9, wherein the computer code for updating the at least one taxonomy further comprises a computer program product for prioritizing the at least one possible network intrusion of the plurality of network intrusions labeled as true positive.

13. A processor for determining computer security threats, the processor including a computer program comprising:

computer code for obtaining a possible intrusions report having indicia of a plurality of possible network intrusions;

computer code for retrieving an actual intrusions report having indicia of at least one actual intrusion from a security network, wherein the security network is at least configured to utilize at least one taxonomy;

computer code for comparing the possible intrusion reports with the actual intrusion reports to determine one or more false positives and one or more true positives; and

computer code for updating the at least one taxonomy with at least one of the false positives and at least one of the true positives.

14. The computer program code of Claim 13, wherein computer code for comparing further comprises:

computer code for labeling indicia of at least one possible network intrusion of a plurality of possible network intrusions as a false positive when at least one actual intrusion counterpart has not occurred; and

computer code for labeling indicia of the at least one possible network intrusion of the plurality of possible network intrusions as true positive when at least one actual intrusion counterpart has occurred.

15. The computer program code of Claim 13, wherein the computer code for updating the at least one taxonomy further comprises a computer program product for sorting the at least one possible network intrusion of the plurality of network intrusions labeled as true positive.

16. The computer program code of Claim 13, wherein the computer code for updating the at least one taxonomy further comprises a computer program product for prioritizing the at

least one possible network intrusion of the plurality of network intrusions labeled as true positive.

17. An apparatus for determining computer security threats at least coupled to an Information Technology (IT) infrastructure, comprising:

a network scanner, wherein the network scanner at least utilizes at least one taxonomy to determine at least one possible intrusion;

an intrusion detector, wherein the intrusion detector at least detects at least one actual intrusion; and

false-positive/true-positive (FPTP) detector, wherein the FPTP detector at least compares the at least one possible intrusion with the at least one actual intrusion in order to update the at least one taxonomy.

18. The apparatus of Claim 17, wherein the FPTP detector further is at least configured to label the at least one possible intrusion as false-positive or true positive.

19. The apparatus of Claim 18, wherein the FPTP detector is at least configured to sort possible intrusions labeled as true positive.

20. The apparatus of Claim 18, wherein the FPTP detector is at least configured to prioritize possible intrusions labeled as true positive.